

FILED

APR 22 2024

Mark C. McCart, Clerk
U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
Information Associated with
ellscooperjppp@gmail.com that is
Stored at a Premises Controlled by Google, LLC.

Case No.

24-mj-291-MTS

FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, Mike Bernier, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

This court has authority to issue this warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). located in the Northern District of California, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violations of:

Code Section	Offense Description
Title 18 U.S.C. 1343	Wire Fraud
Title 19 U.S.C. 1028A	Aggravated Identity Theft

The application is based on these facts:

See Affidavit of Special Agent Michael Bernier, attached hereto.

- ☒ Continued on the attached sheet.
☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Michael Bernier, Special Agent

Printed name and title

Subscribed and sworn to by phone.

Date:

4-22-2024

Judge's signature

City and state: Tulsa, Oklahoma

Mark T. Steele, U.S. Magistrate Judge

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of
Information Associated with
ellscooperjppp@gmail.com that is
Stored at a Premises Controlled by
Google, LLC.**

Case No. _____

FILED UNDER SEAL

Affidavit in Support of an Application for a Search Warrant

I, Special Agent Michael Bernier, being first duly sworn under oath, depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises controlled by Google, LLC, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A-1. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google, LLC, to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachments B-1. Upon receipt of the information described in Section I of Attachments B-1, government-authorized persons will review that information to locate the items described in Section II of Attachment B-1.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I am currently employed as a Senior Special Agent with the Federal Reserve Board – Office of Inspector General (“FRB-OIG”). I am currently assigned to the Washington Field Office where I investigate financial crimes, among other offenses, related to the programs and operations of the Board of Governors of the Federal Reserve System. I have participated in investigations involving the execution of search warrants, including the execution of search warrants on computers and other electronic media. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events, and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for

the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation. Excerpts of documents, emails, and other conversations and correspondence, when referred to herein, are drawn from summaries and may be drawn from draft translations that are subject to revision.

Where statements of others are set forth, except as otherwise noted, they are set forth in substance and in part.

5. Based on my training, experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1343 (Wire Fraud) and 18 U.S.C. § 1028A (Aggravated Identity Theft) have been committed by Bernice Jones, and possibly others. There is also probable cause to search the information described in Attachment A-1 for evidence, instrumentalities, and/or fruits of these crimes, as further described in Attachment B-1.

Jurisdiction

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

7. When the government obtains records pursuant to § 2703, or pursuant to a search warrant, the government is not required to notify the subscriber of the

existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2), and (3). Additionally, the government may obtain an order precluding Google, LLC, from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize the investigation. 18 U.S.C. § 2705(b).

Probable Cause

8. I first became aware of Bernice Jones while investigating fraud related to the Coronavirus Aid, Relief, and Economic Security Act (“CARES Act”), specifically a portion of the CARES Act known as the Paycheck Protection Program (“PPP”), which provided loans to eligible small businesses during the COVID-19 crisis.

9. In April 2021, E.C. unlawfully received a PPP loan in the amount of \$20,833 for an alleged business he/she did not in fact own or operate, which was alleged to have been in the Northern District of Oklahoma (“NDOK”).

10. In October 2023, E.C. explained Bernice Jones aided E.C. in applying for the PPP loans and created false tax documents on his/her behalf which was supplied to PPP lenders. E.C. told me that in exchange for Bernice Jones’ assistance in creating the PPP application and supporting documents, E.C. gave Bernice Jones \$10,000 of the loan proceeds. E.C. also explained that Bernice Jones told E.C. that the loans would later be forgiven.

11. During the investigation, I learned Bernice Jones’s modus operandi was to offer to help people obtain PPP loans in exchange for a portion of the loan proceeds.

My investigation revealed that Bernice Jones aided nearly 40 individuals in obtaining fraudulent PPP loans in the NDOK and elsewhere.

12. E.C. told me E.C. signed the PPP application and once the PPP loan was approved, E.C. confirmed the loan proceeds were deposited into E.C.'s account.

13. For a PPP loan to be forgiven, an applicant must complete and submit SBA Form 3508S, PPP Loan Forgiveness Application to the lender and the SBA. The PPP loan forgiveness application requires the borrower to certify the PPP funds were used for eligible purposes, such as for payroll or business operating expenses.

14. Between April 21, 2021, and August 26, 2021, two PPP Loan Forgiveness Applications were submitted on behalf of E.C. These applications stated that all \$20,833 of the PPP loan proceeds were used for payroll. E.C.'s PPP Loan Forgiveness Applications bore his initials in two places and his signature at the bottom of the form certifying all the information contained on the form was true and correct.

15. E.C. denied ever seeing, initialing, or signing the PPP Loan Forgiveness Applications.

16. The PPP Loan Forgiveness Application submitted on behalf of E.C. listed E.C.'s email address as ellscooperjppp@gmail.com. E.C. stated this was not his email address and he had no knowledge of this email address ever being used or created.

17. My investigation revealed other individuals involved in this scheme also had a gmail.com email addresses with a portion of their names, followed by the letters

“ppp” used. Google records indicate that these email addresses were all set up around the time of their initial PPP applications and I believe they were used to communicate with various PPP lenders.

18. During the investigation, I sent a grand jury subpoena to Google seeking basic subscriber information for several of these “xxxxppp@gmail.com” email addresses. Google records indicated that several of these “xxxxppp@gmail.com” email accounts were set up from the same IP address, which was linked to Macy’s Corporate Services, where Bernice Jones worked at the time.

19. Based upon the totality of circumstances and after reviewing the evidence obtained during this investigation, there is probable cause to believe that Bernice Jones created the email address of ellscooperjppp@gmail.com and then used, without lawful authority, a means of identification, in this case E.C.’s name, initials, and signature, to cause E.C.’s PPP loan to be forgiven.

Background Concerning Email

20. Based on my training and experience, I have learned that Google, LLC, provides a variety of on-line services, including electronic mail (“email”) access, to the public. Google, LLC, allows subscribers to obtain email accounts at the domain name google.com, like the email accounts listed in Attachment A-1. Subscribers obtain an account by registering with Google, LLC. During the registration process, Google, LLC, asks subscribers to provide basic personal information. Therefore, the computers of Google, LLC, are likely to contain stored electronic communications

(including retrieved and unretrieved email for Google, LLC subscribers) and information concerning subscribers and their use of Google, LLC services, such as account access information, email transaction information, and account application information. Based on my training and experience, I know such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

21. A Google, LLC, subscriber can also store with the provider files in addition to emails, such as address books, contact, buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google, LLC. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

22. Based on my training and experience, I know email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Based on my training and experience, I know such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that even if subscribers insert false information to conceal

their identity, this information often provides clues to their identity, location, or illicit activities.

23. Based on my training and experience, I know email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

24. Based on my training and experience, I know in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. Based on my training and experience, I know such

information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

25. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling investigators to establish and prove each element or alternatively, to exclude the innocent from further suspicion. Based on my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at

a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

Information to be Searched and Things to be Seized

26. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Google, LLC. Because the warrant will be served on Google, LLC, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

27. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google, LLC, to disclose to the government digital copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B-1. Upon receipt of the information described in Section I of Attachment B-1, government-authorized persons will review that information to locate the items described in Section II of Attachment B-1.

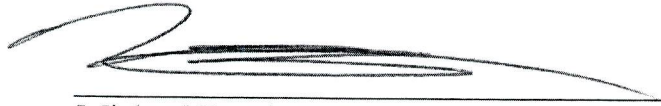
28. In conducting this review, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the account described in Attachment A-1. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with e-mails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but do not contain any searched keywords.

Conclusion

29. Based on the information above, there is probable cause to believe that there is evidence, instrumentalities and/or fruits of the crime, as described in Attachment B-1, of violations of 18 U.S.C. § 1343 (Wire Fraud) and 18 U.S.C. §

1028A (Aggravated Identity Theft) associated with the Google, LLC account described in Attachment A-1.

Respectfully submitted,



Michael Bernier
Senior Special Agent
Federal Reserve Board – OIG

Subscribed and sworn to before me on this 22 day of April, 2024.



MARK T. STEELE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

Property to Be Searched

This warrant applies to information associated with ellscooperjppp@gmail.com from January 1, 2021, to December 31, 2021, that is stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, that accepts legal service of legal process through its Law Enforcement Request System (LERS).

ATTACHMENT B-1

Particular Things to be Seized

I. Information to be disclosed by Google, LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose to the government for each account or identifier listed in Attachment A-1 the following information:

- a. The contents of all emails associated with the account, from January 1, 2021, to December 31, 2021, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.
- f. All transactional information of all activity of the email address described in Attachment A-1 from January 1, 2021, to December 31, 2021, including log files, dates, times, methods of connecting, ports, dial ups, and/or locations;
- g. All images, videos and other files, and associated upload/download date and timestamp, including all available metadata concerning these files associated with the account listed in Attachment A-1;
- h. The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government.

All information described above in Section I that constitutes evidence, and/or instrumentalities of violations of Title 18, United States Code § 1343 (Wire Fraud), and Title 18, United States Code § 1028A (Aggravated Identity Theft), those violations occurring after January 1, 2021, including, for each account or identifier listed on

Attachment A-1:

- a. Communications between the user of ellscooperjppp@gmail.com and PPP lenders on behalf of those involved in fraudulent PPP loan applications;
- b. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- c. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- d. The identity of the person who created or used the email account, including records that help reveal the whereabouts of such person.
- e. The identity of the person(s) who communicated with the email account about matters relating to PPP loan applications, including records that help reveal their whereabouts.
- f. Passwords and encryption keys, and other access information that may be necessary to access the account listed in Attachment A-1 or identifier and other associated account; and

- g. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the account listed in Attachment A-1.

Certificate of Authenticity of Domestic Records
Pursuant to Federal Rules of Evidence 902(11) and 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, LLC., and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google, LLC. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. All records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, LLC, and they were made by Google, LLC. as a regular practice; and

b. Such records were generated by Google, LLC's electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google, LLC, in a manner to ensure that they are true duplicates of the original records; and

2. The process or system is regularly verified by Google, LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature